AO 106 (Rev. 04/10) Application for a Scarch Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION ASSOCIATED WITH ACCOUNT ASSOCIATED
WITH EMAIL ADDRESS rushmemh@gmail.com THAT IS STORED
AT PREMISES CONTROLLED BY GOOGLE, INC.

Case No. 3:18-MJ_156 (TWD)

			,	
	A	PPLICATION FOR A	A SEARCH WARF	RANT
penalty of perjury	that I have reason	to believe that on the fo	ollowing person or p	equest a search warrant and state under property (identify the person or describe the
^{PINETON} ATION AS STORED AT PRE	SSOCIATED WITH A MISES CONTROLLE	CCOUNT ASSOCIATED D BY GOOGLE, INC., AS	WITH EMAIL ADDRE FURTHER DESCRIE	SS rushmermh@gmall.com THAT IS BED IN ATTACHMENT B
located in the	Northern	District of	California	, there is now concealed (identify the
person or describe the See Attachment	: property to be seized) B	i		
,	for the search unde	er Fed. R. Crim. P. 41(c) is (check one or more	ş):
Contraband, fruits of crime, or other items illegally possessed;				
property designed for use, intended for use, or used in committing a crime;				
a person to be arrested or a person who is unlawfully restrained.				
The search is related to a violation of:				
Code S 18 U.S.C. Secti	Code Section 18 U.S.C. Sections 2251 and 2252A Sexual Exploitation of a Child; Distribution, Receipt and Possession of Pornography			
The application is based on these facts: See Attached Affidavit				
Continued on the attached sheet.				
Delayed notice of 90 days (give exact ending date if more than 30 days: 06/23/2018) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.				
ATTESTED TO BY THE APPLICANT IN ACCORDANCE				
WITH THE REQUIREMENTS OF R. 4.1 OF THE Applicant's signature				
FEDERAL RULES OF CRIMINAL PROCEDURE AND			Jenelle Corrine Bringuel, Special Agent FBI	
18 USC SEC. 2703				Printed name and title
Sworn to before me and signed in my presence.				(,)
Date: Much 23, 2018			Gelly Mult. Judge's signature	
			llom This.	
City and state: Syracuse, New York			Hon. Thérèse Wiley Dancks, U.S. Magistrate Judge	

ATTACHMENT B DESCRIPTION OF THE GOOGLE ACCOUNT TO BE SEARCHED AND ITEMS TO BE SEIZED

This warrant applies to information associated with the following Google accounts (the "Subject Google Account") stored at premises owned, maintained, controlled, or operated by Google, Inc. a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043:

a. rushmermh@gmail.com

I. Information to be disclosed by Google, Inc.:

To the extent that the Subject Google Account described in above is within the possession, custody, or control of Google, Inc., including any emails, records, files, logs, or information that has been deleted but is still available to Google, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, Inc. is required to disclose the following information to the government for the Subject Google Account:

- i. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- ii. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- iii. The types of service utilized;
- iv. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

v. All records pertaining to communications between Google, Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251 and 2252A involving Michael H. Rushmer, including, for the Subject Google Account listed above, information pertaining to the following matters:

- i. Visual depictions of Child Pornography as defined in Title 18 United States Code Section
 2256(8);
- ii. The contents of all e-mail, posts or other electronic communications or file stored by or for the Subject Google Account and any associated accounts, and any information associated with those communications or files, such as the source or destination e-mail addresses, I.P. addresses or telephone numbers;
- iii. All records and other information relating to the Subject Google Account and any associated accounts including the following:
 - 1. Subscriber names, user names, screen names, or other identities;
 - 2. Text/SMS/MMS messages;
 - Any other records or evidence relating to the Subject Google Account, including deleted communications, attachments, images, files, videos, the source and destination address (Internet Protocol number, date and time) associated with each communication/posting/comment;
 - 4. All records/logs or other information regarding the identification of the accounts accessed or received by the Subject Google Account, to include full name, physical address, telephone numbers, and other identifiers, records of session times and durations, the date on which the account(s) were created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP

- addresses associated with session/edit/updating times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- All records or other information stored by an individual using the Subject Google
 Account, including address books, contact or buddy lists, calendar data, pictures,
 videos and files;
- All records pertaining to communications between Google, Inc. and any person regarding the Subject Google Account, including contacts with support services and records of action taken;
- 7. Any and all information for Google, Inc. Identification(s) for Subject Google
 Account, to include all subscriber information, such as name and address, telephone
 number, account number, method and manner of payment, date of birth, gender, date
 account created, account status, e-mail address, alternate e-mail address, registration
 IP, date ID registered, and IP addresses associated with session times and dates;
- 8. The contents of any and all e-mails stored in the Subject Google Account;
- 9. Subject Google Account user connection logs, including the following:
 - a. Connection time and date;
 - b.Disconnect time and date;
 - c. Method of connection to system (e.g., SLIP, PPP, Shell);
 - d.Date transfer volume (e.g. bytes);
 - e. The IP address that was used when the user connected to the service;
 - f. Connection information for other systems which user connected via the Subject Google Account, including:
 - i. Connection destination;
 - ii. Connection time and date;

- iii. Disconnect time and date;
- iv. Method of connection to system (e.g. telnet, ftp, http);
- v. Date transfer volume (e.g. bytes);
- vi. Any other relevant routing information:
- 10. Source or destination of any wire or electronic messages sent from or received by the Subject Google Account, and the date, time, and length of the message;
- 11. Any address to which the wire or electronic message was or is to be forwarded from the Subject Google Account or e-mail address.
- 12. Any business records and subscriber information, in any form kept, pertaining to the Subject Google Account, including applications, subscribers' full names, all screen names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;
- 13. All records indicating the services available to subscribers of the Subject Google

 Account; and
- 14. As used above, the terms records, documents, programs, applications, or materials includes records, documents, programs, applications, or materials created, modified, or stored in any form.

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR SEARCH WARRANTS FOR:

[SEE ATTACHMENTS A, B, C, and D HEREIN]

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

JENELLE CORRINE BRINGUEL, being duly sworn, deposes and states:

INTRODUCTION

- 1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI"), and I am empowered by law to investigate and make arrests for offenses enumerated in Title 18, United States Code, Section 2516. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7).
- 2. I have been employed as a Special Agent of the FBI since June 2012 and am currently assigned to the Albany Division, Binghamton Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have participated in the execution of several federal search warrants in child sexual exploitation investigations.
- 3. I am currently investigating Michael H. Rushmer ("Rushmer") and his attempts to persuade a minor to engage in sexually explicit conduct for the purposes of producing a visual depiction of such conduct, using a means and facility of interstate and foreign commerce, and in and affecting such commerce, in violation of Title 18 United States Code, Section 2251(a); knowingly distributing and receiving child pornography using a means and facility of interstate and foreign commerce, and in and

affecting such commerce, in violation of Title 18 United States Code, Section 2252A(a)(2)(A); and knowingly possessing child pornography that has been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, in violation of Title 18 United States Code, Section 2252A(a)(5)(B).

- 4. As will be demonstrated in this affidavit, there is probable cause to believe that evidence will be located: on digital devices seized by the Johnson City Police Department (JCPD) pursuant to a search warrant at Rushmer's residence in Johnson City, NY and digital devices seized from Rushmer upon his arrest by the Federal Bureau of Investigation, which were believed to be in violation of his state pre-trial release conditions (hereafter, the "Subject Electronic Devices," as more fully described in Attachment A); within Rushmer's Google Account, Rushmermh@gmail.com (hereafter, the "Subject Google Account," as more fully described in Attachment B); and within Rushmer's Dropbox Account, michaelandrewdaniel@yahoo.com (hereafter, the "Subject Dropbox Account," as more fully described in Attachment C) relating to violations of Title 18, United States Code 2251 (sexual exploitation of a child), and 2252A (Receipt, Distribution, and/or Possession of Child Pornography), hereafter referred to as the Subject Offenses. I submit this affidavit in support of a search warrant authorizing a search of the Subject Electronic Devices, the Subject Google Account, and the Subject Dropbox Account for evidence of those crimes, as described in Attachment D, including evidence, fruits, and instrumentalities of the Subject Offenses and personally identifying information confirming the owner of the Subject Electronic Devices, Subject Google Account, and Subject Dropbox Account.
- 5. This affidavit and application are made under Fed. R. Crim. P. Rule 41 for authorization to search the subject electronic device and under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require to require Google, Inc. and Dropbox, "providers of electronic communication services" and a "providers of remote computing services" within the meaning of the Electronic Communication Privacy Act, Title 18, United States Code, Chapter 121, to disclose to the government records and other information in its possession, (including the content of the communications; particularly described in Section II of Attachments B and C.) Upon receipt of the information described in Section II of

Attachments B and C, government-authorized persons will review that information to locate the items described in Attachment D.

6. The statements and facts set forth in this affidavit are based in significant part on: my review of written documents obtained from the Johnson City Police Department (JCPD), my review of Michael H. Rushmer's audio and video recorded interview, my observation of a child forensic interview of Victim #1, my review of Rushmer's cell phone, my conservations with Detective James Conrad, JCPD, and my personal training and experiences. Since this Affidavit is being submitted for the limited purposes of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts and circumstances that I believe are necessary to establish probable cause to believe evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2251 and 2252A are presently located on the Subject Electronic Devices, within the Subject Google Account, and within the Subject Dropbox Account.

DEFINITIONS

- 7. The following definitions apply to this affidavit and Attachments A-D:
 - a. "Child Erotica" means materials or other items that are sexually arousing to persons having a sexual interest or desire in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or body positions.
 - b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

- c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).
- d. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- e. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware.
- e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data.

 Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data

security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

- f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.
- i. "Minor" means any person under the age of 18 years. See 18 U.S.C. § 2256(1).
- j. "Sexually explicit conduct" applies to the visual depictions that involve the use of a minor, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated: (a) sexual intercourse (including genital-genital, anal-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d)

- sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. See 18 U.S.C. § 2256(2)(A).
- k. "Visual depictions" include undeveloped film and videotape, as well as data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- 1. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

- 8. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications Records Access."
 - a. Title 18 United States Code, Section 2703(a), provides, in part: "A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure...by a court of

competent jurisdiction...A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications systems for more than one hundred eighty days by the means available under subsection (b) of this section."

- b. Title 18, United States Code, Section 2703(b), provides, in part: "(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure...by a court of competent jurisdiction... (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means by electronic transmission from), a subscriber or customer of such remote computing service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage of computer processing.
- c. The government may also obtain records and other information pertinent to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant issued by a court of competent jurisdiction over the offense under investigation. 18 U.S.C. §2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. §2703(c) (3).
- d. Title 18 United States Code, Section 2711, provides, in part: "As used in this chapter-
 - (1) the terms defined in Section 2510 of this title have, respectively, the definitions given such terms in that section;

- (2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;..."
- e. Title 18, United States Code, Section 2510, provides in part:
 - (8) "contents" when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communications;...
 - (14) "electronic communications system" means any wire, radio,
 electromagnetic, photooptical or photoelectronic facilities for the transmission of
 wire or electronic communications, and any computer facilities or related
 electronic equipment for the electronic storage of such communications;...
 - (15) "Electronic communications service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;...
 - (17) electronic storage" means-
 - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
 - (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication

BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY

- 9. Based on my knowledge, training, and experience, and the experience and training of other law enforcement agents and investigators with whom I have had discussions, I know that electronic devices, including computers and cellular telephones serve different roles or functions with child pornography: production, communication, distribution, and storage.
- 10. Child pornographers can transpose photographic images from a camera into a computerreadable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone,

cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

- 11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within recent years. These drives can store thousands of images at very high resolution.
- 12. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.
- 13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.
- 14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

COLLECTORS OF CHILD PORNOGRAPHY

- 15. Individuals who are interested in child pornography may want to keep the child pornography files they create or receive for additional viewing in the future. Individuals who collect child pornography may go to great lengths to conceal and protect from discovery their collections of illicit materials. They often maintain their collections in the privacy of their homes, on computers, on external hard drives, on cellular telephones, or in other secure locations. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished fantasies, the collector rarely, if ever, disposes of his collection. The collection may be culled and refined, but, over time, the size of the collection tends to increase. Individuals who utilize a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with them over time.
- 16. Individuals who collect child pornography may search for and seek out other like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also may help these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: text messages, video messages, electronic mail, email, bulletin boards, IRC, chat rooms, newsgroups, instant messaging, and other vehicles.
- 17. Individuals who collect child pornography may maintain stories, books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals may keep these materials because of the psychological support they provide.
- 18. Individuals who collect child pornography may keep names, electronic mail addresses, cellular and telephone numbers, or lists of persons who have shared, advertised, or otherwise made known their interest in child pornography or sexual activity with minor children. These contacts may be

maintained as a means of personal referral, exchange, and/or commercial profit. This information may be maintained in the original medium from which it was derived.

BACKGROUND OF THE INVESTIGATION

- 19. On January 24, 2018, your Affiant was advised by Johnson City Police Department (JCPD) that on January 16, 2018, JCPD Detective James Conrad took a complaint from a woman and her son, Victim #1 (a 14 year old male born on XX/XX/2004) regarding Michael H. Rushmer. Victim #1 told Det. Conrad about his experience with Rushmer. He first provided details about Rushmer's residence, including the location and specific details about Rushmer's bedroom. Victim #1 was shown an image of the suspected residence, recognized it to be Rushmer's, and signed the image. Victim #1 explained that Rushmer made him do "inappropriate things," meaning masturbating in Rushmer's bedroom after Rushmer provided him with lubricant. This was referred to as "private time," a phrase which Victim #1 came to recognize as a "secret code" that Rushmer used to signal to Victim #1 that he (Victim #1) would be masturbating later. Victim #1 further explained that he thought he was being video recorded while masturbating because he observed Rushmer conceal his camera phone behind a sign on the shelf in the bedroom. Victim #1 told Det. Conrad that Rushmer did not know that he (Victim #1) saw Rushmer hiding the phone behind the sign. Victim #1 only recalled seeing the camera phone in that place when he (Victim #1) was having "private time." Victim #1 knew it to be Rushmer's phone because Rushmer usually had it with him at all times.
- 20. Victim #1 told Det. Conrad that he was frequently disciplined by Rushmer for being disobedient. Discipline was almost always conducted in Rushmer's bedroom, behind closed curtains, and after Rushmer's three children went to bed. Victim #1 explained that when he was punished, Rushmer would sit on the edge of his bed and ask Victim #1 if he was ready for his spanking. Victim #1 would say "Yes" and be told to systematically strip naked. Once naked, Victim #1 would lie over Rushmer's lap and get spanked on his naked buttocks. Sometimes he was struck by Rushmer's hand, a table tennis paddle, or flat wooden spatula. Victim #1 stated that Rushmer would not only spank his butt, but also

down his leg to the back of his knee and the inside of his thigh. This caused Victim #1 to have redness, bruising, and pain.

- Additionally, Victim #1 talked about 3 separate occasions when Rushmer touched Victim #1's penis. He said it was the only time that he was touched sexually by Rushmer and it occurred during bath time. Victim #1 explained that when he took a bath, Rushmer would enter the room and assist him with getting clean. Victim #1 became agitated and said, "I'm thirteen years old, I can clean myself!" He said that Rushmer put soap on a washcloth and proceeded to scrub his body, specifically his groin, lower stomach, and upper thigh areas. Victim #1 said that his genitals were touched. Lastly, Victim #1 explained how he knew Rushmer, and he was shown a known image of Rushmer. Victim #1 recognized the male in the image to be Rushmer and signed it.
- 22. On January 18, 2018, the JCPD executed a search warrant at Rushmer's residence in Johnson City, NY. During the execution of the search warrant, JCPD seized Rushmer's cellular telephone as well as numerous thumb drives, SD cards, and data storage devices (as listed and fully described as Items #1-12 in Attachment A). Additionally, several other evidentiary items were located, including: 2 table tennis paddles, 1 flat wooden spatula, a "Boy Cave" sign, and 1 bottle of "Swiss Navy Silicone Lubricant." These items are currently in the possession of the JCPD.
- 23. On this same day, an audio and video recorded interview of Rushmer was conducted by the JCPD. During this interview, Rushmer was read his Miranda rights, which he waived (by signing a form) and continued to speak to the JCPD. During this interview, Rushmer admitted to "disciplining" Victim #1 and others. Rushmer explained that he had multiple levels of discipline, but most often chose to spank the children.
- 24. During the interview, Rushmer also stated he had discussed puberty with Victim #1 and that he included masturbation as part of the discussion. Rushmer said that while on a camping vacation with Victim #1, he had used a broom stick to demonstrate masturbation technique. Rushmer said that Victim #1 masturbated while on the camping trip and continued to masturbate when he came over to his house. Rushmer said that he called it "Homework" in order to keep it "PG." Rushmer would also refer to

it (Victim #1 masturbating) as "private time" and said that it occurred in his (Rushmer's) bedroom on the bed. Det. Conrad asked Rushmer if he was recording Victim #1 during "private time" and Rushmer said that it was true. Rushmer went on to say that he had recorded the spankings and Victim #1's "private time" 2-3 times each, and that he was recording them "for my own personal use...pleasure." Rushmer admitted to providing lubricant to Victim #1 to masturbate with, and also stated that he had given Victim #1 a bottle of lubricant for Christmas.

- 25. Rushmer discussed several times (2-3) when he helped Victim #1 bathe. Rushmer described how he was teaching Victim #1 to wash himself, including his private parts. Rushmer said that he had other images of unknown children on his phone. He said that he would get these images from the internet and that he would use his phone to look at those pictures. He said that he has used his phone to view child pornography and has saved his favorites.
- 26. Rushmer signed a Voluntary Consent to Search Form, giving the JCPD permission to search his Motorola cell phone. While in the presence of Rushmer, Det. Conrad viewed the aforementioned camera phone. When doing so, Det. Conrad saw several images of young males, including Victim #1. Specifically, the phone contained numerous images and at least one video of Victim #1 before, during, and after a naked spanking. There were also images of Victim #1 naked and in a bathtub. Det. Conrad also saw numerous other images depicting young, unknown males, including acts of masturbation.
- 27. At the conclusion of his interview, Rushmer was arrested and charged with the following crimes under the New York State Penal Law: Promoting an Obscene Sexual Performance by a Child (PL 263.10), Possessing an Obscene Sexual Performance by a Child (PL 263.11), Unlawful Surveillance in the Second Degree (PL 250.45), Assault in the Second Degree (PL 120.05.2), Endangering the Welfare of a Child (PL 260.10), and Sex Abuse in the Second Degree (PL 130.60.2).
- 28. On February 2, 2018, pursuant to a search warrant issued by Broome County Court Judge Kevin P. Dooley, your Affiant conducted an extraction of Rushmer's Motorola cell phone. As a result of this extraction, your Affiant located several images depicting Victim #1 masturbating on Rushmer's bed.

The images appear to be screenshots of videos that were taken of Victim #1 on at least two occasions. There were also multiple images of the buttocks of Victim #1 and other minor males, wherein the buttocks appeared red, as if they had just been spanked. During a forensic interview of Victim #1 on February 14, 2018, Victim #1 confirmed the aforementioned images were of him.

- 29. Your Affiant observed that the application "Viber" was present on Rushmer's cell phone and is associated with Rushmer's actual cell phone number. The name listed on the Viber account is "Michael." In some Viber chat conversations, Rushmer appears to refer to himself in the third person, sometimes as "Dad" or "Daddy," and portrays himself as an 18 year-old male. Based on the content of the conversations, it appears Rushmer uses this identity with individuals who do not know him outside of the cyber world. In other Viber chat conversations, wherein the individuals have talked with Rushmer via telephone or video chat, Rushmer uses his true identity.
- 30. Your Affiant located a Viber chat conversation between Rushmer and another individual, who is believed to reside in Los Angeles, California. During these chats, the individual refers to Rushmer as "Michael." Among other things, on November 11, 2017, Rushmer distributed several of the screenshot images of Victim #1 masturbating to this individual. During a portion of a conversation with this individual on November 11, 2017, Rushmer states: "anyway tonight I snuck some pics of him when he was masturbating and I'm willing to show you but I need you to PLEASE promise to delete them. I don't want them saved anywhere." Rushmer also told this individual that he had demonstrated to the child depicted in the images he distributed to him how to masturbate by using the end of a broomstick, discussed providing Victim #1 with tissues and lubricant to masturbate with, and stated that he gave Victim #1 a bottle of lubricant for Christmas.
- 31. Rushmer also received hundreds of images depicting child pornography from the aforementioned individual via the Viber chat conversations, which were located on Rushmer's cell phone.

 Two of the images are described as follows:
 - a. IMG-4cbb37bdbaaef1326e01a8b5fad0c761-V.jpg: This image depicts a male

approximately 8 years old without a shirt on performing oral sex on the penis of a nude male child, approximately 8 years old.

b. IMG-3ab3c7523b11abb8cb56d3db3043dd17-V.jpg: This image depicts a nude prepubescent male, approximately 5 years old, masturbating himself.

The individual also sent to Rushmer multiple links to videos, which were not able to be viewed by your Affiant, but whose names are indicative of child pornography.

- 32. During Viber conversations with this same individual, which took place from at least August 2017 through January 2018, Rushmer discusses multiple instances wherein Victim #1 stayed at his house and slept in his bed next to him. He also discusses Victim #1 being spanked and pictures being taken of his red buttocks.
- 33. Your Affiant located multiple SMS conversations on Rushmer's cell phone between Rushmer and other individuals, wherein Rushmer discusses uploading images of the boys after they have been spanked to his Dropbox account. The Dropbox account located on this cellular telephone is associated with email address michaelandrewdaniel@yahoo.com. A preservation letter was served to Dropbox for this account on 3/15/2018.
- 34. Your Affiant observed that the majority of the image files on Rushmer's cellular telephone are or were physically located within Google Photos associated with Google account rushmermh@gmail.com. A preservation letter was served to Google, Inc. for this account on 2/2/2018.
- 35. Rushmer was arrested by the FBI on March 14, 2018, pursuant to a Complaint signed on March 13, 2018 by United States Magistrate Judge Thérèse Wiley Dancks, for violations of Title 18, United States Code, Sections 2251 (sexual exploitation of a child), and 2252A (Receipt, Distribution, and/or Possession of Child Pornography). At the time of this arrest, law enforcement agents went upstairs to Rushmer's bedroom to retrieve additional items of clothing for Rushmer prior to his transport following his arrest and while in his bedroom, member of the FBI noticed two pieces of electronic media in plain view on Rushmer's bed. Law enforcement was aware that it was in violation of Rushmer's state court probation to be in possession of any electronic devices. The two electronic devices were a Blu

Model: Jenny TV 2.8 cell phone and an RCA tablet with an attached keyboard. Rushmer admitted that the cell phone was his and that he had borrowed the tablet, which had internet access. Both of these items were photographed and seized by the JCPD, as they were believed to be in violation of Rushmer's pretrial release conditions.

36. All of the images referenced in this affidavit are available for the Court's inspection upon request.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

- 37. Your Affiant has spoken with law enforcement investigators trained in computer and cellular telephone evidence recovery that have extensive knowledge about the operation of cellular telephones and computer systems including the correct procedures for the seizure and analysis of these systems.
- 38. Based on my knowledge, training, and experience, your Affiant is aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, transferred, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost to the user. Even when files have been deleted, they can be recovered months or years later using specialized forensic tools. This is so because when a person "deletes" a file on a computer or cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- 39. Therefore, deleted files or remnants of deleted files may reside in free space or slack space—that is, in space located on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data or process in a "swap" or "recovery" file.
- 40. Apart from user-generated files, an electronic device may contain electronic evidence of it was used, what it was used for, and more importantly, who used it recently and in the past. This evidence can take the form of operating system configurations, artifacts from operating system or different application operation, file system data structures, and the virtual memory "swap" or paging files.

Similarly, files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache" located on the computer. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

- 41. Although some of the information called for by this search warrant might be found in the form of user-generated documents (such as photographic images and video files), smart phone style cellular telephones can contain other forms of electronic evidence as well:
 - a. Forensic evidence of how the Subject Electronic Device was used, the purpose of its use, who used it, and when, is called for under this request for a search warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Computer file systems can record information about the dates and times files were created and the sequence in which they were created.
 - b. Forensic evidence on an electronic device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence or physical location. For example, registry information, configuration files, user profiles, e-mail address books, "chats," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates and times) may in and of themselves be evidence of who used or controlled the computer or storage medium at a relevant time in question.
 - c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw logical conclusions about how it was used, the purpose of its use, who used it, and when.

- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to the case agents and investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the nature of the evidence described in Attachment D also falls within the scope of the search warrant.
- Searching storage media for the evidence described in the Attachment D may e. require a range of data analysis techniques. It is possible that the storage media will contain files and information that are not called for by the search warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the search warrant is immediately apparent. In most cases, however, such techniques may not yield the evidence described in the search warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the search warrant calls for records of how the Subject Electronic Devices were used, what they were used for, and who used them, it is likely that it will be necessary to thoroughly search the devices to obtain evidence including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a search warrant, a search the Subject Electronic Devices for the things described in this search warrant will likely require a search among the data stored in storage media for the things (including electronic data)

called for by this search warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

SEARCH METHODOLOGY TO BE EMPLOYED: THE SUBJECT ELECTRONIC DEVICES

- 42. The search procedure of electronic and digital data contained on computers, in cellular telephones, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
 - a. examination of all of the data contained in such computer hardware, computer software, cellular telephone, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - c. surveying various file directories and the individual files they contain;
 - d. opening files in order to determine their contents and scanning storage areas;
 - e. performing key word searches to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment D; and
 - f. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment D.

SEARCH METHODOLOGY TO BE EMPLOYED: THE SUBJECT GOOGLE ACCOUNT

43. In order to ensure that Agents search only those Instagram account records described in Attachment A, this affidavit and application for a search warrant seeks authorization to permit employees

of Google, Inc. to assist agents in the execution of this warrant. To further ensure that Agents executing this warrant search only those computer accounts and/or files described in Section II of Attachment B, the following procedures will be implemented:

- a. The search warrant will be presented to Google, Inc. personnel who will be directed to isolate those accounts and files described in Attachment B;
- b. In order to minimize any disruption of computer service to innocent third parties, Google, Inc. employees and law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Attachment B, including an exact duplicate of all information stored in the computer accounts and files described in Attachment B;
- c. Google, Inc. employees will provide the exact duplicate in electronic form of the accounts and files described in Attachment B and all information stored in those accounts and files to the agent who serves this warrant;
- d. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Google, Inc. employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant; and
- e. Law enforcement personnel will then seal the original duplicate of the accounts and files received from Google, Inc. employees and will not further review the original duplicate absent an order of the Court.

SEARCH METHODOLOGY TO BE EMPLOYED: THE SUBJECT DROPBOX ACCOUNT

44. In order to ensure that Agents search only those Instagram account records described in Attachment C, this affidavit and application for a search warrant seeks authorization to permit employees of Dropbox to assist agents in the execution of this warrant. To further ensure that Agents executing this warrant search only those computer accounts and/or files described in Attachment C, the following procedures will be implemented:

- a. The search warrant will be presented to Dropbox personnel who will be directed to isolate those accounts and files described in Attachment C;
- b. In order to minimize any disruption of computer service to innocent third parties,
 Dropbox employees and law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Attachment C, including an exact duplicate of all information stored in the computer accounts and files described in Attachment C;
- c. Dropbox employees will provide the exact duplicate in electronic form of the accounts and files described in Attachment C and all information stored in those accounts and files to the agent who serves this warrant;
- d. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Dropbox employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant; and
- e. Law enforcement personnel will then seal the original duplicate of the accounts and files received from Dropbox employees and will not further review the original duplicate absent an order of the Court.

CONCLUSION

45. Based upon the above information, there is probable cause to believe that evidence of violation of Title 18, United States Code, Sections 2251 (sexual exploitation of a child), and 2252A (Receipt, Distribution, and/or Possession of Child Pornography), as outlined in Attachment D of this Affidavit, will be found within the Subject Electronic Devices, the Subject Google Account, and the Subject Dropbox Account, that are the subjects of this warrant as set forth in Attachments A, B and C respectively. Therefore, based upon the information contained in this affidavit, your Affiant requests this Court issue the attached search warrants authorizing the search of the contents of the Subject Electronic

Devices, the Subject Google Account, and the Subject Dropbox Account set forth in Attachments A, B and C for the items more particularly described in Attachment D.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE AND 18 U.S.C. §§ 2703.

Jenelle Corrine Bringuel

Special Agent

Federal Bureau of Investigation

Sworn to before me this 23rd Day of March 2018.

Hon. Thérèse Wiley Dancks

UNITED STATES MAGISTRATE JUDGE NORTHERN DISTRICT OF NEW YORK

ATTACHMENT A

DESCRIPTION OF THE ELECTRONIC DEVICES TO BE SEARCHED

The following list of items to be searched for evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2251 and 2252A, were seized as a result of the 1/18/2018 search of the Johnson City, NY residence of Michael H. Rushmer, and as a result of the 3/15/2018 arrest of Rushmer, and are currently in the custody of the Johnson City Police Department, Johnson City, NY:

- 1. One (1) Motorola Cell phone, black
- One (1) Red Samsung flip phone Samsung Jitterbug, model SCH-R220, 268435462410949335 A0000040A10949335 FCC ID: A3LSCHR220
- 3. One (1) black Amazon tablet inside folding leather case Amazon model: SV98LN, FCC ID: 2AETF-1013, Lot M605, serial 201-150191
- 4. Three (3) DVDs located in Rushmer's bedroom:
 - A. 1st Side A: Full Screen, Side B (Flipside) Widescreen Hangman's Curse ©2003 TCFHE
 - B. 2nd Sony DVD-R 120m min/4.7 GB, Handwritten "Rescue"
 - C. 3rd Memorex DVD-R 16x 4.7 GB 120 min
- 5. One (1) silver Vivitar memory device Vivitar model VZ30011-SLV, Capacity: 4000mAh, MID#: 2850516
- One (1) 250 GB external hard drive Western Digital model Scorpio Blue, S/N WXW1E51KCSV9, WD2500BPVT, KH25008030134081E37600
- 7. One (1) black smartphone located in dresser drawer Motorola, model XT1031, FCC ID:IHDT56PF3, MEID: A000002CEF3009
- 8. One (1) Targus SD card Targus High Speed SD/SDHC/MMC Micro SD/T-F Card Reader/Writer #5145
- 9. One (1) flash thumbdrive PNY 16GB
- 10. One (1) flash thumbdrive PNY 16GB
- 11. One (1) Blue HP laptop computer HP 2000 Notebook PC Regulatory Model: TPN-1108 or 2000-2b19WM, S/N: 5CG3140YMK, Product: D1E80UA#ABA
- One (1) Acer computer Acer Aspire Model ZRL, 5394 series,
 LXRR902004134081E37600, SNID: 13403325176

- 13. One (1) tablet RCA model RCT6873W42KC, FCC ID: A2HRCT6773W22, IC: 9903A-RCT6773W22 (W/ attached keyboard)
- 14. One (1) cell phone Blu Model: Jenny TV 2.8, FCC ID: YHLBLUJENNYTV28, S/N: 109002101760041, IMEI1: 354278079264416, IMEI2: 354278079616813

ATTACHMENT B DESCRIPTION OF THE GOOGLE ACCOUNT TO BE SEARCHED AND ITEMS TO BE SEIZED

This warrant applies to information associated with the following Google accounts (the "Subject Google Account") stored at premises owned, maintained, controlled, or operated by Google, Inc. a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043:

a. rushmermh@gmail.com

I. Information to be disclosed by Google, Inc.:

To the extent that the Subject Google Account described in above is within the possession, custody, or control of Google, Inc., including any emails, records, files, logs, or information that has been deleted but is still available to Google, Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, Inc. is required to disclose the following information to the government for the Subject Google Account:

- i. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- ii. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- iii. The types of service utilized;
- iv. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

v. All records pertaining to communications between Google, Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251 and 2252A involving Michael H. Rushmer, including, for the Subject Google Account listed above, information pertaining to the following matters:

- i. Visual depictions of Child Pornography as defined in Title 18 United States Code Section
 2256(8);
- ii. The contents of all e-mail, posts or other electronic communications or file stored by or for the Subject Google Account and any associated accounts, and any information associated with those communications or files, such as the source or destination e-mail addresses, I.P. addresses or telephone numbers;
- iii. All records and other information relating to the Subject Google Account and any associated accounts including the following:
 - 1. Subscriber names, user names, screen names, or other identities;
 - 2. Text/SMS/MMS messages;
 - 3. Any other records or evidence relating to the Subject Google Account, including deleted communications, attachments, images, files, videos, the source and destination address (Internet Protocol number, date and time) associated with each communication/posting/comment;
 - 4. All records/logs or other information regarding the identification of the accounts accessed or received by the Subject Google Account, to include full name, physical address, telephone numbers, and other identifiers, records of session times and durations, the date on which the account(s) were created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP

- addresses associated with session/edit/updating times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- 5. All records or other information stored by an individual using the Subject Google
 Account, including address books, contact or buddy lists, calendar data, pictures,
 videos and files;
- All records pertaining to communications between Google, Inc. and any person regarding the Subject Google Account, including contacts with support services and records of action taken;
- 7. Any and all information for Google, Inc. Identification(s) for Subject Google Account, to include all subscriber information, such as name and address, telephone number, account number, method and manner of payment, date of birth, gender, date account created, account status, e-mail address, alternate e-mail address, registration IP, date ID registered, and IP addresses associated with session times and dates;
- 8. The contents of any and all e-mails stored in the Subject Google Account;
- 9. Subject Google Account user connection logs, including the following:
 - a. Connection time and date;
 - b.Disconnect time and date;
 - c. Method of connection to system (e.g., SLIP, PPP, Shell);
 - d.Date transfer volume (e.g. bytes);
 - e. The IP address that was used when the user connected to the service;
 - f. Connection information for other systems which user connected via the Subject Google Account, including:
 - i. Connection destination;
 - ii. Connection time and date;

- iii. Disconnect time and date;
- iv. Method of connection to system (e.g. telnet, ftp, http);
- v. Date transfer volume (e.g. bytes);
- vi. Any other relevant routing information:
- 10. Source or destination of any wire or electronic messages sent from or received by the Subject Google Account, and the date, time, and length of the message;
- 11. Any address to which the wire or electronic message was or is to be forwarded from the Subject Google Account or e-mail address.
- 12. Any business records and subscriber information, in any form kept, pertaining to the Subject Google Account, including applications, subscribers' full names, all screen names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;
- All records indicating the services available to subscribers of the Subject Google Account; and
- 14. As used above, the terms records, documents, programs, applications, or materials includes records, documents, programs, applications, or materials created, modified, or stored in any form.

ATTACHMENT C DESCRIPTION OF THE DROPBOX ACCOUNT TO BE SEARCHED AND ITEMS TO BE SEIZED

The Subject Dropbox Account, that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc. ("Dropbox"), a company headquartered at 333 Brannan Street, San Francisco, CA 94107, and is fully identified and described below as follows:

a. michaelandrewdaniel@yahoo.com

I. Information to be disclosed by Dropbox, Inc.

To the extent that the Subject Dropbox Account described in above is within the possession, custody, or control of Dropbox, including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for the account or identifier listed in above:

- i. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;
- ii. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails "invites" sent or received via Dropbox, and any contact lists.
- iii. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- iv. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- v. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251 and 2252A, including information pertaining to the following matters:

- i. Subscriber information, such as name, email address, zip code and other personal/biographical information;
- ii. Account access information, master and sub account names, user profiles, friends lists, instant messages, grief reports, account creation information, associated IP information for each account use, screen shots of account activity, email transaction information;
- iii. Information relating to transportation, distribution, receipt, and possession of image and movie files that contain child pornography, as that term is defined in 18 U.S.C. § 2256;
- iv. Stored image and video files of any minor engaged in sexually explicit conduct as defined in Title 18, U.S.C. § 2256;
- v. Any information pertinent to identifying any minor or minors portrayed in any image or video found within the accounts, including any correspondence or other communication with said minors;
- vi. Any record of an attempt to commit the listed offenses (18 U.S.C. § 2251 and 2252A) including any correspondence soliciting or otherwise discussing sexually explicit conduct by or with minors, including discussions of or solicitation for meeting with minors and/or for images or videos of minors;
- vii. Any images or videos of minors, such as child erotica, that evidence a sexual interest in children and/or an attempt to produce, receive, or possess child pornography;
- viii. The identity of the person(s) who created or used the user account listed as Subject Dropbox Account;
- ix. The identity of any person(s) who communicated with the user account listed as Subject Dropbox Account about matters relating to the sexual exploitation of children and/or receipt, distribution, or possession of child pornography, as defined in 18 U.S.C. § 2251 and 2252A.

ATTACHMENT D

ITEMS TO BE SEARCHED FOR AND SEIZED FROM ITEMS IN ATTACHMENT A

Items and information that constitute fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251 and 2252A (sexual exploitation of children, and transporting, distributing, receiving, or possessing child pornography,) including:

- a. Any and all visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- b. Internet history including evidence of visits to websites that offer visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256.
- c. Correspondence or other documentation identifying persons transmitting through interstate or foreign commerce, including by mail or computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.
- d. Computer records and evidence identifying who the particular user was who produced, downloaded or possessed any child pornography found on any computer or computer media.
- e. Correspondence and other matter pertaining to the production, purchase, possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in Title 18 United States Code, Section 2256, and evidence that would assist in identifying any victims of the above-referenced criminal offenses, including address books, names, and lists of names and addresses of minors, or other information pertinent to identifying any minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).
- f. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes evidencing an interest in unlawful sexual contact with children, and evidence assisting authorities in identifying any such children.
- g. Any and all records or communications evidencing an intent, or conspiracy, or plan to engage in sexually explicit conduct with a child.
- h. Any and all records or communications with minor children.
- i. Any and all electronically stored records reflecting personal contact and any other activities with minors.

- j. Any notes, writings or other evidence that would assist law enforcement in identifying additional victims of sexual exploitation, witnesses thereto, or other subjects that may have assisted, conspired, or agreed to participate in the sexual exploitation of children.
- k. Records showing the use or ownership of Internet accounts, including evidence of Internet user names, screen names or other Internet user identification.
- Computer software, meaning any and all data, information, instructions, programs, or
 program codes, stored in the form of electronic, magnetic, optical, or other media, which
 is capable of being interpreted by a computer or its related components. Computer
 software may also include data, data fragments, or control characters integral to the
 operation of computer software, such as operating systems software, applications
 software, utility programs, compilers, interpreters, communications software, and other
 programming used or intended to be used to communicate with computer components.
- m. Computer-related documentation that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- n. Computer passwords and data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records.
- o. Documents and records regarding the ownership and/or possession of electronic media being searched.
- p. The authorization includes the search of the electronic media listed on the face of the warrant, for electronic data to include deleted data, remnant data and slack space.